LEAVITT PARTNERS

February 12, 2019

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program NPRM

Information Blocking (pp. 324-502)

Statutory Basis (p. 324)

Section 4004 of the 21st Century Cures Act (Cures Act) added section 3022 of the Public Health Service Act (PHSA) (42 U.S.C. 300jj-52).

- 3022(a)(1) defines practices that constitute information blocking when engaged in by a health care provider, health information technology developer, exchange or network.
- 3022(a)(3) authorizes the Secretary to identify, through notice and comment rulemaking, reasonable and necessary activities that do not constitute information blocking for purposes of the definition set forth in 3022(a)(1).

Legislative Background and Policy Considerations (pp. 324-330)

- Purpose of the Information Blocking Provision
  - The provision was enacted in response to concerns that some individuals and entities are engaging in practices that unreasonably limit the availability and use of electronic health information (EHI) for authorized and permitted purposes, undermining public and private sector investments in the nations health IT infrastructure and frustrate efforts to use modern technologies to improve health care quality and efficiency, accelerate research and innovation, and provide greater value and choice to health care consumers.
  - The information blocking provision defines and creates possible penalties and disincentives for information blocking in broad terms, while working to deter the entire spectrum of practices that unnecessarily impede the flow of EHI or its use to improve health and the delivery of care. The provision applies to the conduct of health care providers, and to health IT developers of certified health IT, exchanges, and networks, and seeks to deter it with substantial penalties, including civil monetary penalties (CMPs), and disincentives for violations. Additionally, developers of health IT certified under the Program are prohibited from information blocking under 3001(c)(5)(D)(i) of the PHSA.
- Policy Considerations and Approach to the Information Blocking Provision
  - Congress authorized the Secretary to identify reasonable and necessary activities that do not constitute information blocking (3022(a)(3) of the PHSA), herein referred to as *exceptions*.
  - The provision also excludes from the definition of information blocking practices that are required by law (section 3022(a)(1) of the PHSA) and clarifies certain other practices that would not be penalized (sections 3022(a)(6) and (7) of the PHSA).
  - Policy Considerations:

- To minimize compliance and other burdens for stakeholders, ONC sought to promote policies that are clear, predictable, and administrable. They also sought to implement the information blocking provision in a way that is sensitive to the legitimate practical challenges that may prevent access, exchange, or use of EHI in certain situations.
- Adhere to Congress's plainly expressed intent to provide a comprehensive response for the information blocking problem.

Relevant Statutory Terms and Provisions (pp. 330-381)

Within this section, ONC outlines how it proposes to interpret certain aspects of the information blocking provision that they believe to be ambiguous, incomplete, or that provide the Secretary with discretion.

- Required by Law:
  - refers specifically to interferences with access, exchange, or use of EHI that are explicitly required by state or federal law.
- Health Care Providers, Health IT Developers, Exchanges, and Networks
  - Section 3022(a)(1) of the PHSA refers to four classes of individuals and entities that may engage in information blocking and which include: health care providers, health IT developers of certified health IT, networks and exchanges.
  - ONC proposes to adopt definitions of these terms to provide clarity regarding the types of individuals and entities to whom the information blocking provision applies. ONC will refer to these individuals and entities as "actors".
  - *Health Care Providers:*
    - HCP is defined in section 3000(3) of the PHSA, ONC proposes to adopt that definition, and notes that while it is different than the definition of HCP under HIPAA, they are considering adjusting the information blocking definition of HCP to cover all individuals and entities covered by the HIPAA definition. ONC seeks comment on whether this approach would be justified.
  - *Health IT Developers of Certified Health IT:*
    - Section 3022(a)(1)(B) of the PHSA defines information blocking, in part, by reference to the conduct of "health information technology developers." Title XX of the PHSA does not define "health information technology developer, therefore ONC interpreted section 3022(a)(1)(B) in light of specific authority provided to OIG in section 3022(b)(1)(A) and (b)(2). Which discusses developers, networks, and exchanges in terms of an individual or entity, specifically cross-referencing section 3022(b)(1)(A). Sections 3022(b)(1) and (b)(1)(A) state that OIG may investigate information blocking claims regarding a health information technology developer of certified HIT or other entity offering certified HIT. Together, the sections make clear that the information blocking provisions and OIG's authority extend to individuals *or* entities that develop *or* offer certified HIT. The information blocking provisions would be implicated by any practice engaged in by an individual or entity the develops or offers certified HIT that is likely to interfere with the access, exchange, or use of EGU, including practices associated with *any* of the developer or offeror's HIT products that have *not* been certified under the Program.
    - ONC proposes to adopt a definition of health information technology (IT) developer of certified health IT for the purposes of interpretation and

enforcement of the information blocking provisions, including those regulatory provisions proposed under 45 CFR Part 171.

- ONC is also considering additional approaches to help ensure that developers or offerors of certified HIT remain subject to the information blocking provision for an appropriate period of time after leaving the Program.
    - One way to achieve this would be to define "health IT developer of certified health IT" as including developers and offerors of certified HIT that continue to store EHI that was previously stored in health IT certified in the Program.
    - Alternatively, ONC is considering whether developers and offerors of certified HIT should remain subject to the provisions after leaving the program, namely, that the information blocking provision should apply for a specific period of time after the developer or offeror no longer has any health IT certified in the program.

- *Networks and Exchanges:*
    - ONC proposes to define these terms, as they are not defined in the information blocking provision or in any other relevant statutory provisions.
    - Health Information Network:
        - ONC proposes a functional definition of this term that focuses on the role of these actors in the health information ecosystem. The defining attribute of a HIN is that it *enables, facilitates, or controls the movement of information between or among different individuals or entities that are unaffiliated.* ONC proposes that two parties are affiliated if one has the power to control the other, or if both parties are under the common control or ownership of a common owner.
        - An actor could be considered a HIN if it performs any or any combination of the following activities:
            - Actor would be a HIN if it were to determine, oversee, administer, control, or substantially influence policies or agreements that define the business, operational, technical, or other conditions or requirements that enable or facilitate the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.
            - Actor would be a HIN if it were to provide, manage, control, or substantially influence any technology or service that enables or facilitates the access, exchange or use of EHI between or among two or more unaffiliated individuals or entities.
            - The proposed definition would also encompass an individual or entity that does not directly enable, facilitate, or control the movement of information, but nonetheless exercises control or substantial influence over the policies, technology, or services of a network.
    - Health Information Exchange:
        - ONC proposes to define a HIE as an individual or entity that enables, access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes.

        - If an HIE facilitates the access, exchange, or use of EHI for more than a narrowly defined set of purposes, then it may be both an HIE and HIN.
    - Electronic Health Information (EHI)[1]
    - Interests Promoted by the Information Blocking Provision
        - Access, Exchange, and Use of EHI[2]
        - Interoperability Elements[3]
    - Practices that May Implicate the Information Blocking Provision[4]
        - To meet the definition or information blocking, a practice must be *likely to interfere with, prevent, or materially discourage* access, exchange, or use of EHI.
        - Prevention, Material Discouragement, and Other Interference[5]
        - Likelihood of Interference[6]
            - Observational Health Information[7]
            - Purposes for Which Information May be Needed[8]
            - Control Over Essential Interoperability Elements; Other Circumstances of Reliance or Dependence[9]
        - Examples of Practices Likely to Interfere with Access, Exchange, or Use of EHI[10]
            - Restrictions on Access, Exchange, or Use
            - Limiting or Restricting the Interoperability of Health IT[11]
            - Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-enabled Care Delivery[12]
            - Rent-seeking and Other Opportunistic Pricing Practices[13]
            - Non-Standard Implementation Practices[14]
    - Applicability of Exceptions[15]:
        - Reasonable and Necessary Activities

[1] P. 344

[2] P. 350

[3] P. 353

[4] P. 353

[5] P. 355

[6] P. 356

[7] P. 357

[8] P. 360

[9] P. 361

[10] P. 364

[11] P. 367

[12] P. 370

[13] P. 374

[14] P. 377

[15] P. 379

- Section 3022(a)(3) authorizes the Secretary to identify, through notice and comment rulemaking, reasonable and necessary *activities* that do not constitute information blocking for purposes of the definition set out in section 3022(a)(1).
- The Cures Act identifies at section 3022(a)(1) *practices* that contravene the definition of information blocking. Thus, conduct that implicates the information blocking provision and that does not fall within one of the exceptions (described below), or does not meet all conditions for an exception, would be considered a "practice." Conduct that falls within an exception and meets all the applicable conditions for that exception would be considered an "activity."

▪ Treatment of Different Types of Actors[16]

- The proposed exceptions would apply to health care providers, health IT developers of certified HIT, HIEs, and HINs who engage in certain practices covered by an exception, provided that all applicable conditions of the exception are satisfied at all relevant times and for each practice for which the exception is sought.

Proposed Exceptions to the Information Blocking Provision (pp. 381-497)

ONC is proposing seven exceptions to the information blocking provision. The proposed exceptions are based on three related policy considerations:

- Each exception is limited to certain activities that clearly advance the aims of the information blocking provision.
- Each exception addresses a significant risk that regulated actors will not engage in these beneficial activities because of uncertainty concerning the breadth or applicability of the information blocking provision' and
- Each exception is subject to strict conditions to ensure that it is limited to activities that are reasonable and necessary.

<u>Exceptions:</u>

- Preventing Harm:
  - ONC proposes to establish an exception to the information blocking provision for practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. The exception and corresponding conditions are set forth in the proposed regulation text in §171.201.
  - Patient harm risks that would be cognizable under this exception:
    - To qualify for this proposed exception, an actor's practice must respond to a risk that is cognizable under this exception.
  - Risk of corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record (EHR).
    - The exception may apply to practices that prevent harm arising from corrupted or inaccurate EHI being recorded or incorporated in a patient's EHR.

[16] P. 380

        - This recognized risk is limited to corruption and inaccuracies caused by performance and technical issues affecting HIT.
        - This recognized risk does not extend to purported accuracy issues arising from the incompleteness of a patient's EHR generally.
        - The risk that the EHI a given health care provider holds for a given patient may not be a perfectly complete record of that patient's health or care will not be recognized as being sufficient to support an actor qualifying for this exception in the face of a claim of information blocking.
        - This exception would not recognize an actor's conduct in not providing access, exchange, or use of a patient's EHR on the basis that the patient's failure to consent to the disclosure of substance abuse treatment information made the patient's record incomplete and thus inaccurate.
    - Risk of misidentifying a patient or patient's EHI
        - This exception may apply to practices that are designed to promote data quality and integrity to support HIT applications properly identifying and matching patient records or EHI.
        - An actor's response to this risk would need to be no broader than necessary to mitigate the risk of harm arising from the potentially misidentified record or misattributed data.
    - Determination by a licensed HCP that the disclosure of EHI is reasonably likely to endanger life or physical safety.
        - This exception may permit certain restrictions on the disclosure of an individual's EHI in circumstances where a licensed HCP has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to engender the life or physician safety of the patient or another person.
            - This would include the situation where a covered entity elected not to treat a person as the personal representative of an individual in situations of potential abuse or endangerment, including in accordance with 45 CFR § 164.502(g)(5).
            - ONC requests comment on whether the categories of harm described capture the full range of safety risks that might arise directly from accessing, exchanging, or using EHI, as well as whether it should consider other types of patient safety risks related to data quality and integrity concerns, or that may have a less proximate connection to EGHI, but that could provide a reasonable and necessary basis for an actor to restrict or otherwise impede access, exchange, or use of EHI in appropriate circumstances.
    - Reasonable belief that practice was necessary to directly and substantially reduce the likelihood of harm.
        - To qualify for this exception, an actor must have had a reasonable belief that the practice or practices will directly and substantially reduce the likelihood of harm to a patient or another person. As discussed above, the type of risk must also be cognizable under this exception. An actor could meet this condition in two ways.
    - Qualifying organizational policy.
        - An actor could demonstrate that the practices it engaged in were consistent with an organizational policy that was objectively reasonable and no broader than

necessary for the type of patient safety risks at issue. An actor's policy would need to satisfy the following requirements:
    - The policy must be in writing;
    - The policy must have been developed with meaningful input from clinical, technical and other appropriate staff or others who have expertise or insight relevant to the risk of harm that the policy addresses;
    - The policy must have been implemented in a consistent and non-discriminatory manner; and
    - The policy must be no broader than necessary for the specific risk or type of risk at issue.
  - Qualifying individualized finding:
    - In circumstances where there are not comprehensive formal policies, or ones that do not anticipate all of the potential risks of harm that could arise, in lieu of demonstrating that a practice conformed to the actor's policies and that the policies met the conditions described above, the actor could justify the practice or practices directly by making a finding in each case, based on the particularized facts and circumstances, that the practice is necessary and no broader than necessary to mitigate the risk of harm.
    - The actor would need to show that the practices were approved on a case-by-case basis by an individual with direct knowledge of the relevant facts and circumstances and who had relevant clinical, technical, or other appropriate expertise.
    - A licensed HCP's independent and individualized judgment about the safety of the actor's patients or other persons would be entitled to substantial deference under this proposed exception.
- Promoting the Privacy of EHI:
  - ONC proposes to establish an exception to the information blocking provision for practices that are reasonable and necessary to protect the privacy of an individual's EHI, provided certain conditions are met.
  - The exception and corresponding conditions are set forth in the proposed regulation text in § 171.202.
  - Any practice engaged in protecting the privacy of an individual's EHI must be consistent with applicable laws related to health information privacy, including HIPAA's Privacy Rule, as well as other applicable laws and regulations, such as the HITECH Act, 42 CFR part 2, and state laws.
  - This exception is structured with discrete "sub-exceptions", and an actor's practice must qualify for a sub-exception in order to be covered by this exception. The four proposed sub-exceptions are:
    - Not providing access, exchange, or use or EHI when a state or federal law requires that a condition be satisfied before an actor provides access, exchange, or used of EHI, and the condition is not satisfied (proposed in § 171.202(b));
    - Not providing access, exchange, or use of EHI when the actor is a health IT developer of certified HIT that is not covered by the HIPAA Privacy Rule in respect to a practice (proposed in § 171.202(c));
    - A covered entity, or a business associate on behalf of a covered entity, denying an individual's request for access to their electronic PHI in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3) (proposed § 171.202(d)); and

        - Not providing access, exchange, or use of EHI pursuant to an individual's request, in certain situations (proposed in § 171.202(e)).
    - An actor would need to satisfy at least one sub-exception in order that a purportedly privacy-protective practice that interferes with access, exchange, or use of EHI not be subject to the information blocking provision.
    - Specific terminology used for the purposes of this proposed exception[17]
    - Interaction between information blocking, the exception for promoting the privacy of EHI, and the HIPAA Privacy Rule.
        - Intent is that the information blocking provision does not conflict with the HIPAA Privacy Rule.
        - Note that the information blocking provision may operate to require that actors provide access, exchange, or use of EHI in situations that HIPAA does not.
    - Promoting patient privacy rights
        - ONC has structured the privacy exception to ensure that actors can engage in reasonable and necessary practices that advance the privacy interests of individuals.
        - ONC notes that an individual's expressed privacy preferences will not be controlling in all cases, and that an actor will not be able to rely on an individual's expressed privacy preference in circumstances where the access, exchange, or use is required by law.
        - ONC proposes that the proposed sub-exception in § 171.202(e) would generally permit an actor to give effect to individuals' expressed privacy preferences, including their desire not to permit access, exchange, or use of their EHI.
        - Want to ensure that the privacy exception is tailored to ensure that protection of an individual's privacy is not used as a pretext for information blocking.
    - Privacy Practices Required by Law
        - Because the information blocking provision excludes from the definition of information blocking practices that are required by law (Section 3022(a)(1) of the PHSA), privacy-protective practices that are required by law do not implicate the information blocking provision and do not require coverage from an exception.
    - Sub-exception to proposed privacy exception: Precondition not satisfied
        - ONC proposes to establish a sub-exception to the information blocking provision that recognizes that an actor will not be engaging in information blocking if an actor does not provide access, exchange, or use of EHI because a necessary precondition required by law has not been satisfied.
        - This exception will apply to all instances where an actor's ability to provide access, exchange, or use is "controlled" by a legal obligation to satisfy a condition, or multiple conditions, prior to providing that access, exchange, or use.
        - To be covered by this exception the actor must comply with provisions that are tailored to the implicated privacy laws (various state privacy laws, federal privacy laws, etc.)[18]
    - Conditions to be met to qualify for the sub-exception

[17] P. 397

[18] Pp. 403-407

- An actor can qualify, in part, for this sub-exception by implementing and conforming to organizational policies and procedures that identify the criteria to be used by the actor, and as applicable, the steps that the actor will take, in order to satisfy the precondition.
- An alternative basis on which to qualify, is to permit actors to instead document, on a case-by-case basis, the criteria used by the actor to determine when the precondition will be satisfied, any criteria that were not met, and the reason why the criteria were not met.
- ONC also proposes that if the precondition that an actor purports to have been satisfied relies on the provision of consent or authorization from an individual, it is a condition of this sub-exception that the actor must have done all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide that consent or authorization.

- Organizational policies and procedures
  - If an actor seeks to qualify for the sub-exception, in part, by implementing and conforming to organizational policies and procedures, such policies and procedures must be in writing, and specify the criteria used by the actor, and, if applicable, the steps the actor will take, in order to satisfy the precondition relied on by the actor to not provide access, exchange, or use of EHI.
    - An actor would only qualify for this sub-exception if it has followed its processes and policies.
    - The actor's privacy policies and procedures would need to identify criteria for making a "minimum necessary" determination for both routine and non-routine disclosures and requests, including identifying the circumstances under which disclosing the entire medical record is reasonably necessary.
      - For actors that are covered entities or business associates, the development of policies and procedures for the making of minimum necessary determinations for requesting, using, and disclosing PHI is already a requirement of the HIPAA Privacy Rule, so ONC expects that actors will already have such policies and procedures in place.
    - An actor's policies and procedures must have been implemented to ensure that an actor can only satisfy the condition by reference to privacy policies and practices that individuals in fact benefit from, and not ones that have been documented but not applied.
- Documenting criteria and rationale
  - If an actor's practice does not conform to an actor's organizational policies or procedures as required by § 171.202(b)(1), ONC proposes that an actor seek to qualify for the sub-exception, in part, by documenting how it reached its decision that it would not provide access, use, or exchange of EHI on the basis that the precondition had not been satisfied. Such a determination would occur on a case-by-case basis.
  - The record created by the actor must identify the criteria used by the actor to determine when the precondition is satisfied.
- Meaningful opportunity to provide consent or authorization

        - If the precondition that an actor purports to have satisfied relies on the provision of a consent or authorization from an individual, it is a condition of this sub-exception to provide the individual with a meaningful opportunity to provide that consent or authorization.
        - A meaningful opportunity would ordinarily require that an actor provide the individual with a legally compliant consent form; make a reasonable effort to inform an individual that he or she has the right to consent to the disclosure of their EHI; and provide the individual with sufficient information and educational material (commensurate with the circumstances of the disclosure).
        - It would be best practice for an actor to also inform the individual about the revocability of any consent given, if and as provided in the relevant state or federal privacy law, and the actor's processes for acting on any revocation.
        - The actor must not have improperly encouraged or induced the individual to not provide the consent or authorization.
    - Practice must be tailored to the specific privacy risk or interest being addressed.
        - An actor's privacy-protective practice must be tailored to the specific privacy risks that the practice actually addresses.
    - Practice must be implemented in a consistent and non-discriminatory manner
        - This condition would provide basic assurance that the purported privacy practice is directly related to a specific privacy risks and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.
        - This condition requires that the actor's privacy-protective practices must be based on objective criteria that apply uniformly for all substantially similar privacy risks.
    - Sub-exception to proposed privacy exception: Health IT developer of certified health IT not covered by HIPAA
        - The sub-exception proposed in § 171.202(b) recognizes as reasonable and necessary the activities engaged in by actors consistent with the controls placed on access, exchange, or use of EHI by federal and state privacy laws.
        - ONC proposes to establish a sub-exception to the information blocking provision that would apply to actors that are health IT developers of certified health IT but not regulated by the HIPAA Privacy Rule in respect to the operation of the actor's health IT product or service (referred to hereafter as "non-covered actors).
        - Where a health IT developer of certified health IT offers a health IT product or service not regulated by the HIPAA Privacy Rule, such product or service is subject to the information blocking provision.
        - ONC wants to ensure that non-covered actors that engage in reasonable and necessary privacy-protective practices that interfere with the access, exchange, or use of EHI can seek coverage under this proposed sub-exception.
        - As a threshold requirement of this sub-exception, the actor's practice of interfering with access, exchange, or use of EHI must comply with any applicable state or federal laws.
    - Practice must implement privacy policy
        - The practice engaged in by the non-covered actor—the interference with access, exchange, or use of EHI—must also implement a process described in the actor's organizational privacy policy.

        - This requires that a non-covered actor must have documented in detail in its organizational privacy policy the processes and procedures that the actor will use to determine when the actor will not provide access, exchange, or use of EHI.
        - The non-covered actor's practice must implement its documented organizational privacy policy.
    - Practice must have been disclosed to its users
        - A non-covered actor that seeks to benefit from the proposed sub-exception must also ensure that it has previously disclosed the privacy-protective practice to the individuals and entities that use, or will use, the health IT>
        - ONC expects that non-covered actors will seek to satisfy this condition by using a privacy notice.
        - Notice must be meaningful, and regard will be paid to whether the disclosure was in plain language and conspicuous, including whether the disclosure was located in a place, and presented in a manner, that is accessible and obvious to the individuals and entities that use, or will use, the health IT.
        - To qualify for this sub-exception, a non-covered actor would not be required to disclose its organizational privacy policy to its customers or the public generally, but rather, only need to describe, with sufficient detail and precision to be readily understood by uses or the non-covered actor's health IT, the privacy-protective practices that the non-covered actor has adopted and will observe.
    - Practice must be tailored to privacy risk and implemented in a non-discriminatory manner
        - In order for a practice to qualify for this sub-exception, an actor's practice must be tailored to the specific privacy risks that the practice actually addresses and must be implemented in a consistent and non-discriminatory manner.
    - Sub-exception to proposed privacy exception: Denial of an individual's request for their electronic PHI in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3)
        - ONC proposes a limited sub-exception to the information blocking provision that would permit a covered entity or business associate to deny an individual's request for access to their PHI in circumstances provided under 45 CFR 164.524(a)(1), (2), and (3).
    - Sub-exception to proposed privacy exception: Respecting an individual's request not to share information.
        - ONC proposes to establish an exception to the information blocking provision that would, in certain circumstances, permit an actor not to provide access, exchange, or use of EHI is an individual has specifically requested that the actor not do so.
        - This sub-exception is proposed in § 171.202(e).
        - This would not apply under circumstances where an actor interferes with a use or disclosure of EHI that is required by law, including when EHI is required by the Secretary to enforce HIPAA under 45 CFR 164.502(a)(2)(ii) and 45 CFR 164.502(a)(4)(i).
        - This sub-exception would permit an actor not to share EHI if the following conditions are met:
            - The individual made the request to the actor not to have his or her EHI access, exchanged, or use;

- The individual's request was initiated by the individual without any improper encouragement or inducement by the actor; and
- The actor or its agent documents the request within a reasonable time period.

- Promoting the Security of EHI
  - ONC proposes to establish an exception to the information blocking provision that would permit actors to engage in practice that are reasonable and necessary to promote the security of EHI, subject to certain conditions.
  - Without this exception, actors may be reluctant to implement security measures or engage in other activities that are reasonable and necessary for safeguarding the confidentiality, integrity, and availability of EHI.
  - Cures directs the National Coordinator, in consultation with the HHS Office of Civil Rights (OCR), to issue guidance on common "security barriers" that prevent the trusted exchange of EHI.
  - Cures also seeks to promote the security of EHI, which it defines as an element of interoperability and a target area for the policy development to be undertaken by the Health Information Technology Advisory Committee.
    - The inclusion of these provisions promotes broader access, exchange, and use of EHI while at the same time continuing to promote the confidentiality, integrity, and availability of EHI through security practices that are appropriate and tailored to identified vulnerabilities and risks.
  - To qualify for this exception, an actor's conduct must satisfy threshold conditions.
    - The particular security-related practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI, implemented consistently and in a non-discriminatory manner, and tailored to identified security risks.
    - This proposed exception would not apply to all practices that purport to secure EHI, rather, it will only be available when the actor's security-based practice satisfies the conditions applicable to this exception.
      - The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI.
        - This proposed exception would not apply to any practices that are not directly related to safeguarding the security of EHI.
        - ONC will consider whether and to what extent the practice directly addressed specific security risks or concerns, and whether the practice served any other purposes, and if so, whether those purposes were merely incidental o the overriding security purpose or provided an objectively distinct, non-security-related rationale for engaging in the practice.
      - The practice must be tailored to the specific security risk being addressed.
        - To qualify for this exception, an actor's security-related practice must be tailored to specific security risks that the practice actually addressed.
        - ONC proposes that, to the extent the practice implements and organizational security policy, the policy must align with applicable consensus-based standards or best practices for responding to these types of incidents.

- Practice must be implemented in a consistent and non-discriminatory manner.
    - The actor's practice must have been implemented in a consistent and non-discriminatory manner for the proposed exception to qualify.
- Practices that implement an organizational security policy.
    - It is important that actors develop and implement organizational policies that secure EHI.
    - ONC proposes that, where an actor has documented security policies that align with applicable consensus-based standards, and where the policies are implemented in a consistent and non-discriminatory manner, a practice's conformity with such policies would provide a degree of assurance that the practice was reasonable and necessary to address specific security risks and thus should not constitute information blocking.
    - Conversely, a practice that went beyond an actor's established policies or practices by imposing security controls that were not documented, would not qualify under this condition (although the actor may be able to qualify under the alternative basis for practices that do not implement a security policy).
    - To support a presumption that a practice conducted pursuant to the actor's security policy was reasonable, the policy would have to meet the following conditions:
        - Risks identified and assessed: the actor's security policy must be informed by an assessment of the security risks facing the actor. A good risk assessment would use an approach consistent with industry standards,[19] and would incorporate elements such as threat and vulnerability analysis, data collection, security measures, likelihood of occurrence, impact, level of risk, and final reporting.[20]
        - Consensus-based standards or best practice guidance: the actor's policy must align with one or more applicable consensus-based standards or best practice guidance.
        - Objective timeframes and other parameters: the actor's security policy must provide objective timeframes and common terminology used for identifying, responding to, and addressing security incidents.
- Practices that do not implement an organizational security policy.
    - ONC expects that most security practices engaged in by an actor will implement an organizational policy.

[19] See OCR, Guidance on Risk Analysis, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidancerisk-analysis/index.html?language=es.

[20] ONC and OCR have jointly launched the HHS HIPAA Security Risk Assessment (SRA) Tool, https://www.healthit.gov/providers-professionals/security-risk-assessment-tool.

    - If a practice does that does not implement an organizational policy is to qualify for this exception, it must meet certain conditions:
        - The actor's practice must, based on the particularized facts and circumstances, be necessary to mitigate the security risk.

- Recovering Costs Reasonably Incurred
    - ONC proposes to establish an exception to the information blocking provision that would permit the recovery of certain costs reasonably incurred to provide access, exchange, or use of EHI.
    - The exception and corresponding conditions are set forth in the proposed regulation text in § 171.204.
    - ONC interprets the definition of information blocking to include *any* fee that is likely to interfere with the access, exchange, or used of EHI.
    - ONC proposes to establish an exception that would permit the recovery of certain costs that it believes are unlikely to present information blocking concerns and would generally promote innovation, competition, and consumer welfare, provided certain conditions are met.
    - This exception would only apply to the recovery of certain costs and only when the actor's methods for recovering such costs comply with certain conditions at all relevant times. These conditions would require that the costs the actor recovered were reasonably incurred and did not reflect costs that are speculative or subjective. Actors would be required to allocate costs in an appropriate manner and to use objective and permissible criteria when charging fees to recover those costs. Further, the exception would not apply to certain fees, such as those based on the profit or revenue associated with the use of EHI (either being earned by the actor, or that could be realized by another individual or entity) that exceed the actor's reasonable costs for providing access, exchange, or use of EHI. Finally, the exception would provide additional conditions applicable to fees charged in connection with: (1) the certified APIs described in § 170.404; and (2) the EHI export capability proposed in § 170.315(b)(10) for the purposes of switching health IT or to provide patients their electronic health information.
        - Requirement that costs be reasonably incurred: any costs the actor seeks to recover must have been reasonably incurred to provide the relevant interoperability elements to enable access, exchange, or use of EHI.
        - Method for recovering costs: to qualify for the exception, the method by which the actor seeks to recover its costs must be reasonable and non-discriminatory. This would require that the actor base its recovery of costs on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. Also, the method by which the actor recovers its costs must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged. Furthermore, the method by which the actor recovers its costs must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported. The exception would not apply if the method by which the actor recovers its costs is based, in any part, on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that

facilitates competition with the actor. Lastly, the method by which the actor recovers its costs must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of EHI, including the secondary use of such information that *exceeds* the actor's reasonable costs for providing access, exchange, or use of EHI.

- Costs Specifically Calculated: Certain costs should be explicitly excluded from this exception, regardless of the method for recovering the costs. Those include:
  - Costs due to non-standard design or implementation choices: this exception would not permit the recovery of any cost that the actor incurred due to the HIT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI.
  - Subject or Speculative Costs: this exception is limited to the recovery of costs that an actor *actually* incurred to provide the relevant interoperability element or group of elements (which may comprise either products or services). This exception would not permit the recovery of certain types of costs that are subjective or speculative (*e.g.*, costs associated with intangible assets, and "opportunity costs").
- Fee Prohibited by 45 CFR 164.524(c)(4)
  - This exception would not apply to fees prohibited by 45 CFR 164.524(c)(4). The HIPAA Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (*e.g.*, CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual.
  - The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by state law.
- Individual Electronic Access:
  - This exception would not apply if the actor charged a fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's EHI.
- Export and Portability of EHI maintained in EHR systems:
  - The definition of information blocking specifically mentions transitions between health IT systems and the export of complete information tests as protected forms of access, exchange, and use.
  - ONC proposes that fees charged for the export, conversion, or migration of data from and EHR technology would not qualify for the exception unless they also meet two additional conditions:

        - HIT developers and developers of certified HIT would, for purposes of this exception, be precluded from charging a fee to perform an export of EHI via the capability of HIT certified to the proposed 2015 Edition "EHI export" certification criterion (§ 170.315(b)(1)) for the purposes of switching HIT systems or to provide patients their EHI.
        - This exception would not apply to a fee to export or convert data from and EHR technology unless such fee was agreed to in writing at the time the technology was acquired, meaning when the EHR developer and the customer entered into a contract or license agreement for the EHR technology.
    - Compliance with the Condition of Certification Specific to API Technology Suppliers and API data providers
        - HIT developers of certified HIT subject to the API Condition of Certification must comply with all requirements of that condition for all practices and at all relevant times in order to qualify for this exception.
    - Application of the Exception to individual practices:
        - Conditions of this exception, including those governing the methodology and criteria by which an actor calculates and distributes its costs, must be satisfied for *each and every fee* that an actor charges to a customer, requestor, or other person.
- Responding to Requests that are Infeasible
    - ONC proposes to establish an exception to the information blocking provision that would permit an actor to decline to provide access, exchange, or use of EHI in a manner that is infeasible, provided certain conditions are met.
    - This exception and corresponding conditions are set forth in the proposed regulation text in § 171.205.
    - The exception would permit an actor to decline a request in narrowly-defined circumstances when doing so would be infeasible (or impossible) and when the actor otherwise did all that it could reasonably do under the circumstances to facilitate the alternative means of accessing, exchanging, and using the EHI.
        - Infeasibility of Request: ONC proposes a two-step test that an actor would need to meet in order to demonstrate that a request was infeasible.
            - Complying with the request would impose a substantial burden on the actor
            - The burden imposed on the actor would be plainly unreasonable under the circumstances
        - Duty to timely respond and provide reasonable cooperation: an actor would have to show that it satisfied several additional conditions:
            - The actor must have timely responded to all requests related to access, exchange, and use of EHI, including but not limited to requests to establish connections and to provide interoperability elements. Further, for any request that the actor claims was infeasible, the actor must have provided the requestor with a detailed written explanation of the reasons why the actor could not accommodate the request. Finally, the actor must have worked with the requesting party in a timely manner to

identify and provide a reasonable alternative means of accessing, exchanging, or using the EHI, as applicable. The actor's failure to meet any of these conditions would disqualify the actor from the exception and could also be evidence that the actor knew that it was engaging in practices that contravened the information blocking provision.

- Licensing of Interoperability Elements on Reasonable and Non-discriminatory Terms
  - ONC proposes an exception to the information blocking provision that would permit actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms, provided certain criteria are met.
  - This exception and corresponding conditions are set forth in the proposed regulation text in § 141.206.
    - This licensing requirement would apply in both vertical and horizontal relationships.
  - Reasonable and Non-Discriminatory (RAND) Terms
    - Any terms upon which an actor licenses interoperability elements must be RAND.
    - To qualify, an actor must license requested interoperability elements on RAND terms. To comply with this condition, any terms or conditions under which the actor discloses or allows the use of interoperability elements must meet several requirements. These requirements apply to both price terms (*e.g.*, royalties and license fees) and other terms, such as conditions or limitations on access to interoperability elements for the purposes for which they can be used. These conditions include:
      - Responding to requests: upon receiving a request to license or use interoperability elements, an actor would be required to respond to the requestor within 10 business days from the receipt of the request. An actor would be required to respond to the requestor within 10 business days from the receipt of the request by: (1) negotiating with the requestor in a RAND fashion to identify the interoperability elements that are needed; and (2) offering an appropriate license with RAND terms, consistent with its other obligations under this exception.
      - Scope of rights: the actor must license the requested interoperability elements with all rights necessary to access and use the interoperability elements for the following purposes, as applicable:
        - All rights necessary to access and use the interoperability elements for the purpose of developing products or services that are interoperable with the actor's health IT or with health IT under the actor's control and/or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control. These rights would include the right to incorporate and use the interoperability elements in the licensee's own technology to the extent necessary to accomplish this purpose.
        - All rights necessary to market, offer, and distribute the interoperable products and services described above to potential customers and users, including the right to copy or disclose the interoperability elements as necessary to accomplish this purpose.

        - All rights necessary to enable the use of the interoperable products or services in production environments, including using the interoperability elements to access and enable the exchange and use of electronic health information.
    - Reasonable Royalty: if an actor charges a royalty for the use of interoperability elements, the royalty base and rate must be reasonable.
    - Non-discriminatory terms: the terms on which an actor licenses and otherwise provides interoperability elements must be non-discriminatory.
    - Collateral Terms: Five additional conditions that would reinforce the requirements of the exception:
        - The actor must not require the licensee or its agents or contractors to not compete with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development.
        - The actor must not require the licensee or its agents or contractors to deal exclusively with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development.
        - The actor must not require the licensee or its agents or contractors to obtain additional licenses, products, or services that are not related or can be unbundled from the requested interoperability elements.
        - The actor must not condition the use of interoperability elements on a requirement or agreement to license, grant, assign, or transfer the licensee's own IP to the actor.
        - The actor must not condition the use of interoperability elements on a requirement or agreement to pay a fee of any kind whatsoever unless the fee meets either the narrowly crafted condition to this exception for a reasonable royalty, or, alternatively, the fee satisfies the separate exception proposed in § 171.204, which permits the recovery of certain costs reasonably incurred.
    - Non-disclosure agreement:
        - An actor would be permitted under this exception to require a licensee to agree to a confidentiality or non-disclosure agreement (NDA) to protect the actor's trade secrets, provided that the NDA is no broader than necessary to prevent the unauthorized disclosure of the actor's trade secrets. Further, the actor would have to identify (in the NDA) the specific information that it claims as trade secrets, and that such information would have to meet definition of a trade secret under applicable law
- Additional Requirements Relating to the Provision of Interoperability Elements:
    - An actor's practice would need to comply with additional conditions that ensure that actors who license interoperability elements on RAND terms

do not engage in separate practices that impede the use of those elements or otherwise undermine the intent to this exception.
    - An actor would not qualify for this exception if it engaged in a practice that had the purpose or effect of impeding the efficient use o the interoperability elements to access, exchange, or use EHI for any permissible purpose; or the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.
    - An actor cannot avail itself of this exception if, having license the interoperability elements, the actor makes changes to the elements or its technology that "break" compatibility or otherwise degrade the performance or interoperability of the licensee's products or services.
- Compliance with Conditions of Certification
    - Health IT developers of certified health IT who are subject to the Conditions of Certification proposed in §§ 170.402, 170.403, and 170.404 must comply with all requirements of those Conditions of Certification for all practices and at all relevant times.

- Maintaining and Improving Health IT Performance:
    - ONC proposes an exception to the information blocking provision for certain practices that are reasonable and necessary to maintain and improve the overall performance of health IT, provided certain conditions are met.
    - The proposed exception would recognize as reasonable and necessary the practice of an actor making health IT under its control temporarily unavailable to maintain or improve the health IT.
    - The exception and corresponding conditions are set forth in the proposed regulation text in § 171.207.
    - This exception would apply to the unavailability of HIT occasioned by both planned and unplanned maintenance and improvements.
    - Conditions that must be satisfied at all relevant times to qualify for the exception:
        - Unavailability of health IT must be for no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable:
            - Any unavailability of health IT must be for a period of time no longer than necessary to achieve the maintenance or improvement purpose for which the health IT is made unavailable.
        - Unavailability of health IT for maintenance or improvements must be implemented in a consistent and non-discriminatory manner
            - any unavailability of health IT occasioned by the conduct of maintenance or improvements must be implemented in a consistent and non-discriminatory manner.
        - Unavailability of health IT for maintenance or improvements must be agreed.
            - the unavailability of health IT due to maintenance or improvements initiated by a health IT developer of certified health IT, HIE, or HIN, must be agreed to by the individual or entity to whom the health IT is supplied.
                - This proposed condition of this exception only applies when the unavailability of health IT is caused by a health IT developer of certified health IT, HIE, or HIN.

    - This condition does not apply when health IT is made unavailable for maintenance or improvements at the initiative of a recipient (or customer) of health IT, because in that case, the unavailability has, for the purpose of this exception, nothing to do with the supplier.
  - Interaction with Preventing Harm and Promoting Security Exceptions
    - When health IT is made unavailable for maintenance or improvements aimed at preventing harm to a patient or other person, or securing EHI, an actor must comply with the conditions specified in proposed § 171.201 or § 171.203 respectively, in order to qualify for an exception to the information blocking provision.

Additional Exceptions – Request for Information (pp. 497-499)

- Exception for Complying with Common Agreement for Trusted Exchange
  - To support full network-to-network exchange of EHI, section 3001(c)(9)(A) of the PHSA, added by section 4003 of the Cures Act, directs the National Coordinator to convene public-private partnerships to develop or support a trusted exchange framework (Trusted Exchange Framework), including a common agreement for a common set of rules for trusted exchange between HINs (Common Agreement).
    - ONC is considering whether to propose a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement. It would do so by providing protection if there are practices that are expressly required by the Common Agreement, or that are necessary to implement such requirements, that might implicate the information blocking provision and would not qualify for another exception.
- New Exceptions:
  - ONC welcomes comment on any potential new exceptions it should consider for future rulemaking.

Complaint Process (pp. 499-501)

- Section 3022(d)(3)(A) of the PHSA directs the National Coordinator to implement a standardized process for the public to submit reports on claims of health information blocking. Such reports could be submitted regarding any practice by health care providers, health IT developers, exchanges, or networks that may constitute information blocking under section 3022(a). These practices include, but are not limited to, health IT products or developers of such products (or other entities offering such products to health care providers) not being interoperable or resulting in information blocking; and false statements by developers of certified health IT that they have not engaged in information blocking. Section 3022(d)(3)(B) further requires that this complaint process provide for the collection of such information as the originating institution, location, type of transaction, system and version, timestamp, terminating institution, locations, system and version, failure notice, and other related information.

Disincentives for Health Care Providers – RFI (pp. 501-502)

- Section 3022(b)(2)(B) of the PHSA provides that any health care provider determined by the OIG to have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable federal law, as the Secretary sets forth through notice and comment rulemaking.